PKI Disclosure Statements

ChamberSign France CA3 RGS

Authentification_1etoile

Purpose of the Document:	This document describes the terms and conditions for the use of RGS* level natural person authentication certificates issued by the Certification authority ChamberSign France "ChamberSign France CA3". It is the PKI disclosure statement for end-users certificates attached to this hierarchy
Version	00
Date of release	21/02/2025
Diffusion	Public

Warning

Statement types	Statement descriptions
TSP contact info :	All information relating to the ChamberSign France Certification Authority is available on its website https://www.chambersign.fr/. It can be contacted in the following ways: - By post at the following address: Le Cours du Midi, 10, Cours de Verdun Rambaud 69002 Lyon. - By telephone on 08 92 23 02 52 (€0.45 including VAT per minute in mainland France only) - By e-mail by completing the contact form for the department concerned, accessible via the following French link: https://www.chambersign.fr/p-nous-contacter/ Certificates may be revoked by authorized persons via their revocation area, accessible via the following link: https://support.chambersign.fr/revocation-certificat-electronique/ Finally, any questions or comments about these Certificates Policies can be sent by email to the following address: qualite@chambersign.fr.
Certificate type, validation procedures and usage :	A cryptographic media is proposed by the CA or chosen by the holder. However, this media must comply with the relevant requirements of RGS level 1*. The subject contractually commits to ChamberSign France on compliance. Keys pairs of subject are not escrowed or backuped by the CA. Cryptographic media containing the keys pairs of subject must ensure the function of authentication for the legitimate subject only and protect the key pair against unauthorized use by third parties. The use is the authentication of subjects from remote servers or to other people. It may be authentication through access control to a server or application, or origin authentication data within email. Authentication is not a signature on a legal sense because it does not mean that the subject gives his consent to the data exchanged (the non-repudiation guarantee is not available). If the subject's environment is under control and is trusted, then there is no specific security impacts to consider. However, if the environment used is not deemed safe, it is the subject to ensure that the operation he is doing is an authentication operation. If the subject of the environment is not deemed safe, it is recommended that it ensures both that the key pair is used only for authentication certificate which was issued to him and secondly that the application implementing the authentication mechanisms uses the fair practice of the certificate.

Moreover, ChamberSign France may be forced to issue test certificates. These test certificates are identified as such in their DN by the explicit mention TEST. They are covered by any warranty by ChamberSign France and they must never be used for purposes other than for testing purposes. In the late stages of testing, these certificates are revoked.

Certificates issued in accordance to these Terms of service contain the following OID: 1.2.250.1.96.1.8.1.10

Field	Content
DN	encoded in UTF8String
countryName	ISO on 2 letters (cf. ISO3166-1) of the country of the competent authority with which the entity is officially registered (commercial court, ministry,...)
organizationName	official name of the entity (name of the head office)
organizationalUnitName	National identifier of the structure among : • For entities based in Metropolitan France and DOM : 0002 <<SIRET number on 14 characters>> • For entities based in New Caledonia: S540 <<RIDET number on 9 characters maximum>>. • For other entities based in a country of the European community: S<<ISO3166-1 country code on 3 digits>> <<intra-community VAT number on 14 characters maximum>> The field can be iterated 3 times
organizationIdentifier	The official registration number of the provider according to [EN_319_412-1] clause 5.1.4. In France, this registration number can also be the prefix "SI:FR-" followed by the SIREN or SIRET number Identifier of the entity with which the holder is linked: • VAT<country code>-<intra-community VAT number>. • NTR<country code>-<SIREN number>
locality	city where the subject is located
surName	Subject name

givenName	First name1(,First name2,First name3,…) The different first names are mentioned in the order indicated during registration. When several first names are indicated, they are concatenated and separated by commas. Example: Michel,Paul-Auguste.
commonName	Corresponds to the concatenation of the givenName and surname fields separated by a space. Example: Pauline BIENCONNUE
title	where applicable, depending on the position of the subject within his or her organization
serialNumber	4-digit sequential number used to handle cases of multiple certificates for one and the same person. By default, the value of this attribute is “0100”. If a subject with all other DN attributes identical (countryName, organizationName, organizationIdentifier, organizationalUnitName and commonName) has already been registered, the value of the serialNumber attribute for the new subject changes to “0101” and so on.

Certificate request files, containing the key pair to be certified, are sealed using the corresponding key pair.

Information regarding the structure on which the subject is attached are subject to verification upon registration (existence, validity, ...).

The identity of the subject is verified through the verification documents including a certified copy of which is provided by the subject.

Following validation of the certificate request file by the registration function, the process consists to give to the subject the pulic key signed by the CA: generation of the key pair, under control of the subject, into a cryptographic media (software or hardware) chosen by the subject, sending the key pair to the certificate generation function, downloading the generated certificate on the media.

The certificate is accepted implicitely by the subject or the person in charge of certificates by downloading the certificate.

	The first renewal, if authorized by the regulations at the time of expiry date of the certificate to be renewed, can be performed online if it takes place before the expiry date of the corresponding certificate. The subject or the person in charge of certificates confirms that information related to certificate renewal is always accurate. The next renewal is carried out following the initial registration procedure. The renewal after revocation is carried out according to the initial registration procedure. The main cause for the issuance of a new certificate and the corresponding key pair is the end of validity of the certificate. The validity period of certificates provided by ChamberSign France is three (3) years. The key pairs must be effectively periodically renewed to minimize the risk of cryptographic attack. A renewal can also be made in advance, following a declared event or incident by the subject or the person in charge of certificates, the most frequent being the loss, theft or malfunction of cryptographic media. In this case the renewal is, for the subject, to redo an initial application. A modification of the information contained in the certificate also involves the issuance of a new certificate (with renewal of the key pair). In all these cases, the issuance of a new certificate is carried out in the same way as the initial issuance process. Only the registration phase may differ for a renewal. Only a few documents may not be requested (deed of appointment of the legal representative for example). Any revocation request is subject to an applicant authentication and verification of his authority. There can be no certificate suspension. Only the final certificate revocation can be performed. ChamberSign France ensures the availability of the revocation status at any time and beyond the certificate validity period by implementing the following measures: • Publication without a time limit of revoked certificates in the CRL published. The following circumstances may cause the revocation of a certificate: • the certificate key pair is lost, stolen, unusable (malfunction of support), compromised or suspected compromise (request of the subject itself); • information or attributes of the subject contained in the certificate is no longer valid or no more consistent with the intended use of the certificate, this before the normal expiry of the certificate; • cryptographic algorithms used are obsolete and are no longer considered safe;

	• it has been shown that the subject has not respected the applicable terms of use of the certificate; • the CA certificate is revoked (which results in the revocation of certificates signed by the corresponding key pair); • the subject no longer meets the professional requirements (cessation of activity, death). The causes of revocation are never published. Revocation requests are processed within 24 hours after receiving the request, 7 days / 7 (weekends and holidays included if the revocation is processed by the subject the person in charge of certificates or natural person mandated to represent the subject), excluding consecutive revocations to requests for modification of the subject data. The revocation management function is available round the clock, 7 days a 7. The maximum duration of downtime per interruption (failure or maintenance) of the revocation management function is 2 hours (business days). The maximum total duration of downtime per month of revocation management function is 16h (business days).
Reliance limits :	Use of the Subject's Private Key and Certificate must remain strictly limited to authentication services. The Client agrees that ChamberSign France retains documents for proof of identification control of the subject for the periods provided in the Certificate Policy and the documents relating to the conclusion of this contract. The event logs are kept on site for a period of thirty (30) days if the Client has made a request in paper format. After their generation, they are archived and kept for eleven (11) years. The original registration files are archived with archivers third party for a period of eleven (11) years from the issuance of the certificate. If Client’s request to obtain a copy of the registration dossier, the Client will be charged the corresponding cost. Certificates and CRLs are archived for a period of five (5) years after their expiry. If the Client wishes that the registration files, the Certificates or the CRLs are kept for a longer period of archiving, he will have to make the necessary ones and to take the cost himself at his charge.
Obligations of subscribers:	The Client and its Legal Representative undertake to respect the provisions of the PDS. The Client and its Legal Representative are responsible for the management of Certificates issued to employees, delegates or agents of Client under the subscription agreement and undertake to ensure that any Certificate’s subject violating obligations under the Terms and that no fraud or error is committed. As such, the Client and its

	Legal Representative will ensure in particular that the leader: - communicates via the contact point identified herein, the information to create the certificate and any changes during the duration of the certificate; - respects the revocation procedure described in Article 9 Revocation of the Certificate; - keeps secret and secure way, confidential data and the physical support of the Certificate. The Client and its Legal Representative undertake to provide all relevant information, accurate and updated for the creation and management of certificates. The Client and its Legal Representative undertake to inform the home Registration Authority of any changes to information contained in the certificate by mail with the required supporting documents without delay. The previous certificate will be revoked and a new certificate containing the updated information will be issued. The Client and his Legal Representative shall ensure that the certificate is used under the exclusive control of his Subject, and undertake to inform ChamberSign or the relevant Registration Office in the event of loss, theft, compromise of the certificate or disclosure of the PIN code or password. Where applicable, he undertakes to no longer use the compromised Certificate, and ChamberSign reserves the right to revoke it latter. The Client and its Legal Representative vouch for the accuracy of the information provided and completeness of the supporting documents required for registration of the Certificates. The Client and its Legal Representative recognize and accept that the information provided thereunder are kept and used by ChamberSign France to manage certificates as provided by law and in particular those relating to the protection of personal data. The Client and its Legal Representative acknowledge being informed of the conditions of installation of Certificates ChamberSign France. In particular, the certificate is the subject of a tutorial available on the website of ChamberSign France. The Client and its Legal Representative choose hardware and software offering security in line with their requirements for the installation and protection of Certificates and physical media. The Subject is responsible for verifying the validity of the certificate and the conformity of its use.

Certificate status checking obligations of relying parties:	Stakeholders verify and respect the use for which a Certificate has been issued. Stakeholders check that the Certificate issued by ChamberSign France is referenced at the level of security and for the trusted service required by the application. For each of the Certificates in the Certification chain, from the Holder's Certificate to the root Certification Authority, the Stakeholders verify the status of the Certificate and in particular the digital signature of ChamberSign France, issuer of the Certificate in question, and check the validity of this Certificate. Stakeholders verify and comply with these obligations as expressed in the applicable Certification Policy. Stakeholders must verify the non-revocation of the certificates on which they will base their confidence. This verification is done by checking the CRL available via the website ChamberSign France at https://support.chambersign.fr/lcr/. The revoked certificates are still present in the CRL even after their original expiration date. The service is available 24 hours / 24 and 7 days / 7 via the website ChamberSign France. The maximum duration of downtime per interruption (failure or maintenance) of the information based on the status of certificates is 8 hours. The maximum total duration of downtime per month of the information function of the status of certificates is 32 hours. Stakeholders must verify that the certificates on which they are going to base their trust have not been revoked. This verification is done by consulting the CRLs available via the CSF website at the following address: https://support.chambersign.fr/lcr/, or by querying the online certificate status service (OCSP) which includes a “certificate revoked” response after the certificate's end of life date. Revoked certificates remain in the CRL even after their original expiry date. The following circumstances may result in the revocation of a certificate covered by these PDS: - the certificate's private key is lost, stolen, unusable (device malfunction), compromised or suspected of being compromised (request by the certificate holder himself) ; - the information contained in the certificate is no longer valid or no longer consistent with the intended use of the certificate, before the normal expiration of the certificate ; - the cryptographic algorithms used are obsolete and are no longer considered secure ; - it has been demonstrated that the holder has not complied with the applicable terms and conditions of use of the certificate ; - the CA certificate is revoked (which leads to the revocation of the certificates signed by the corresponding private

	key) ; - the person responsible for the certificate has changed and has not been replaced The causes of revocation are never published.
Limited warranty and disclaimer / Limitation of liability:	ChamberSign France is responsible for the compliance of its Certificate Policy, the requirements issued by the model of CPS. ChamberSign France assumes any harmful consequences resulting from non-compliance with its Certificate Policy by itself or one of its components. ChamberSign France acknowledges liability in case of proven misconduct or negligence of itself or one of its components, whatever their nature and severity, which would result in reading, alteration or misuse of personal data subjects for fraudulent purposes, these data are contained in transit or in the Certificates management applications. ChamberSign France is responsible for maintaining the security level of the technical infrastructure on which it relies to provide its services. ChamberSign France can not be held liable for damage caused by use of the Certificate beyond the limits of the authorized use. Responsibility of ChamberSign France can not be held liable for inaccurate information due to false declarations, false documents or no information of changes in the situation of the Subject, the Legal Representative, or natural person mandated to represent the subject when creating or valid certificate, which the false declaration, false documents or the omission is intentional or not. ChamberSign France assumes no obligation or responsibility for the consequences of delays in transmission, alteration, errors or loss of any email, letter or document, signed or otherwise authenticated. ChamberSign France does not in any way be held responsible for the contents of files or transactions signed or authenticated using the certificate, the Client and the subject is only vis-a-vis third parties responsible for the content of these shipments.

	ChamberSign France will in no case liable for indirect damage such as, for example, any financial or commercial loss, loss of income or operating, finding their origin or resulting subscription or inherent in the use of certificates issued by ChamberSign France. ChamberSign France assumes no obligation or liability for the use by the Holder of a Certificate not in accordance with the PDS, especially regarding the validity of control procedures certificate during a transaction. Otherwise, ChamberSign France can not be responsible for phenomena related to normal wear of computer media, including the deterioration of the information given on the said media due to the influence of magnetic fields. ChamberSign France can not be held liable for such damage related to a disruption or malfunction of services and applications for Certificates User. If the Legal Representative has acquired one or more physical media, ChamberSign France is responsible only for their physical deliverance. Due to the constant evolution of technology and levels of security attached to the standards in force in case of malfunction of the physical media or its associated driver software, the Client must request revocation of the Certificate. ChamberSign France can not be responsible for the use of subject Private Key, who has personal responsibility. Any damage related to the Compromise of the Private Key is the Client. ChamberSign France can not be held liable due to illicit use of the Certificate once the Client, the Legal Representative, the Certification Agent or the subject has not made a revocation request in accordance with the Terms.
Applicable agreements, SPC, PO Box:	The applicable certification policy is published at the following address: https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
Privacy policy:	See Appendix 1
Refund policy:	ChamberSign France has subscribed for all of the physical, material and immaterial arising from its business insurance covering the consequences of professional liability. Under the insurance contract by ChamberSign France, and the limits and conditions of this contract, the subject

	will benefit from the replacement of lost or stolen certificate.
Applicable law, complaints and dispute resolution:	In case of difficulty of any kind and before any legal proceedings, the parties undertake to implement a non court dispute resolution procedure. The parties agree to meet at the initiative of either party within eight days from receipt of the letter requesting non court meeting. The agenda is set by the party that takes the initiative of non court meeting. The decisions, if adopted by mutual agreement, guaranteed. This clause is legally independent of this Agreement. It continues to apply despite the possible invalidity, resolution, termination or extinction of these contractual relationships. Otherwise, jurisdiction is assigned to the French courts. These Terms are governed by French law. This is so for the substantive rules and the rules of form and this, notwithstanding the places of performance of the substantive or accessory obligations.
TSP and repository licenses, trust marks and audit:	Certificates issued are qualified at the RGS. User may verify the Root Certificate's fingerprint on the secure website https://pc.chambersign.fr/ca3/index.html or by contacting ChamberSign France by phone at 08 92 23 02 52 from metropolitan France (rate available on the ChamberSign France website) from 9:00 am to 12:30 pm and from 1:30 pm to 6:00 pm, except on Fridays at 5:00 pm, on business days. CRL publishing points are: http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_RGS.crl The CA certificate can be downloaded the following address: https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.cer

	The LCR certificate profiles comply with the ETSI EN 319 412 standard. The list of certificates of compliance with the standards is available on the website at the following address: https://www.chambersign.fr/attestations-de-conformite-certification/ The national trusted list is available via the following link: https://cyber.gouv.fr/la-liste-nationale-de-confiance

1.1.APPENDIX 1. PROTECTION OF PERSONAL DATA

1. PERSONAL DATA

1.2.1.1 PROCESSING OF PERSONAL DATA

1. ChamberSign believes that privacy is fundamental to our relationship with you. It is important to us to protect your privacy and that of your partners and collaborators, with regard to the information that you entrust to us.

2. The main purpose of this article is to inform you about the collection and use of your personal data by ChamberSign, in the context of the provision of our services. The data collected by Chambersign is strictly necessary to provide our services.

3. In accordance with the European Regulation n°2016/679, known as the General Data Protection Regulation (RGPD) and the provisions of Law n° 78-17 of January 6, 1978, as amended, relating to information technology, files and freedoms, ChamberSign acts as a Data Controller concerning the collection and processing of personal data of users of its services. We are therefore responsible for compliance with the obligations arising from this text. These provisions do not apply to the processing of personal data that ChamberSign may perform as a subcontractor.

4. As such, the personal data collected by ChamberSign France for the purpose of issuing and maintaining Certificates are identity data (last name, first name), as well as data related to your professional life (job title, department, professional email). ChamberSign France does not collect any sensitive data such as religion, trade union membership, racial and ethnic origins, criminal convictions or health-related data.

5. ChamberSign France collects personal data from its customers and processes it for the purposes inherent in providing its certification services. The processing of your personal data is therefore based on the respect of our contractual obligations. In this context, we collect your personal data in order to provide you with our services, to manage and follow the life cycle of your certificates and bi-keys (issuance, retention, renewal, revocation) to manage access to and the functioning of your Customer Area or to follow our commercial relationship.

6. The information collected is mandatory. Otherwise, Chambersign France will not be able to provide certification services. The data collected is only intended for use by ChamberSign France's authorized departments. Some of this data may be transferred to ChamberSign's subcontractors, who follow the same privacy policy as ChamberSign. The data transmitted will be strictly limited to the needs defined for the execution of the subcontractor's mission.

7. The subcontractors likely to access your personal data are as follows:
    - Advertising agency based in France, responsible for the transfer of the newsletter by email;

- Digital Services Company (ESN) based in France, responsible for providing the first level of technical support;
- IT hosting company based in France, responsible for hosting the ChamberSign website;
- Archiving company based in France responsible for archiving certificate application files for the legally required period of time;
- Chambers of Commerce and Industry that are ChamberSign partners responsible for verifying identities, validating files and issuing certificates;
- Public and private entities that are ChamberSign partners responsible for issuing certificates for their employees, customers or members;
- ChamberSign's trusted service provider partner responsible for providing the signature of the parties when ordering certificates;
- Cheque management service provider responsible for cashing cheques;
- ChamberSign's trusted service provider partner responsible for verifying the validity of identity documents

8. ChamberSign France does not and will not sell your personal data. The data processed by ChamberSign France is not transferred outside the European Union.

9. In accordance with our standards and the present PDS, we keep your data for eleven (11) years from the date of issue of the certificate.

10. In accordance with current regulations, you have the right to access, rectify, delete, limit the processing of your personal data, object to their use, as well as a right to portability and to define guidelines on the fate of your data after your death.

11. In order to exercise your rights, you may contact us by mail with a copy of a signed identification document at the following address ChamberSign France - 10, Cours de Verdun Rambaud - 69002 LYON or by email at the following address: rgpd@chambersign.fr, being specified that to secure the authentication, the sending of an electronically signed email is preferred. In the absence of an electronic signature, ChamberSign France will authenticate the applicant by any appropriate means, in order to avoid any disclosure of personal data.

12. In case of reasonable doubt, ChamberSign reserves the right to ask you to provide a copy of your identity document by a secure means, it being specified that this document will not be reused for purposes other than your authentication in the context of the request to exercise your rights, and will not be kept beyond the time required for this purpose.

13. To learn more about the use of your data and the exercise of your rights under the French Data Protection Act and the RGPD, you can consult our data protection policy, which is an integral part of these PDS, or contact our Data Protection Officer at rgpd@chambersign.fr.

14. Furthermore, we inform you that you have the right to lodge a complaint with a control authority (CNIL): https://www.cnil.fr/fr/agir.

2. Cookies

1. When User visits our website, cookies are sent to User's computer, tablet or cell phone, subject to the expression of his or her consent from the cookie management banner displayed on the first page visited, and allowing him or her to accept all cookies, refuse them all, or customize their collection. In order to better protect User from cookies and to

understand their usefulness, ChamberSign has adopted a Cookie Usage Policy which is an integral part of these PDS and which User is encouraged to review.